MATH 314 Fall 2023 - Class Notes

10/19/2023

Scribe: Zachary Wagenmann

Summary: In todays class we went over Modular Exponentiation and Fermat's Theorem

Notes:

- Modular Exponentiation

1. Idea: Write b in binary
2. Use repeated squaring to calculate $a^{2i} \pmod m$ for all powers of 2 showing up in b
3. Multiply together the terms corresponding to 1's in binary expansion

1. Ex: $17^{162} \pmod{19}$

   Write 162 in binary $162 = 128 + 32 + 2 = 10100010$

2. Compute $17^{2^7}17^{2^5}17^{2^1}$

   $17^2 = -2^2 = 4 \pmod{19}$

$17^4 = 4^2 = 16 \pmod{19}$

$17^8 = 16^2 = -3^2 = 9 \pmod{19}$

$17^{16} = 9^2 = 81 = 5 \pmod{19}$

$17^{32} = 5^2 = 25 = 6 \pmod{19}$

$17^{64} = 6^2 = 36 = 17 \pmod{19}$

$17^{128} = 17^2 = 4 \pmod{19}$

$17^{162} = 17^{128+32+2} = 17^{128} * 7^{32} * 7^2 = 4 * 6 * 4 \pmod{19} = 1 \pmod{19}$

- Fermat's Little Theorem

If p is a prime and a is any number not divisable by p then $a^{p-1} = 1 \pmod p$
Ex. $p = 3a = 7$ $7^{3-1} = 7^2 = 49 = 1 \pmod 3$
$p = 7a = 3$
$3^{7-1} = 3^6 = 9^3 = 729 = 1 \pmod 7$